What cybersecurity schemes are required within the EU

Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht - German-US Dialogue on IT Security taking organised by Teletrust

SAN FRANCISCO, USA
APRIL 2018

Ladies and gentlemen,

On behalf of ENISA, I would like to thank you for the opportunity to address you today.

In my intervention, I plan to discuss emerging cybersecurity challenges that stem from the digitisation of Industry and the ever-increasing use of Internet of Things (IoT). I will start by highlighting the threats related to these technological challenges and will explain how new technologies have changed the scene and opened up novel opportunities. I will also share ENISA's views on how EU legislation and the proposed Cybersecurity Act will pave the way for a more open, secure and trustworthy digital market.

The industrial sector as we know it is changing.

We are nowadays witnesses to a new Industrial Revolution, which in Europe we call Industry 4.0. The main drivers of this revolution is the use of novel IoT technologies, big data analytics, robotics, artificial intelligence, 3D printing and cloud computing, to name a few. This digitisation of industries empowers the introduction of self-managed, automated processes and leads to more integrated and smart value chains.

Industry 4.0 involves intelligent, interconnected cyber-physical systems that automate all phases of industrial operations, spanning from design and manufacturing to operation, supply chain and service maintenance. This cross-system, integrated use of IoT-based technologies will naturally lead to higher productivity and competitiveness, more flexibility and will instigate new business models.

A 2015 study[1] estimated that, in the next 5 years, digitisation of products and services will add more than 110 billion euros of industry revenue per year in Europe. In Germany[2], digitisation of industry is expected to bring up to 8% of productivity growth by 2025 and a revenue growth of about 30 billion euros per year. It will also lead to a 6% increase in employment.

But all of these forecasted benefits will remain just numbers on a sheet of paper, unless cybersecurity is seriously taken under consideration. The introduction of these novel IoT technologies and the increased connectivity promoted in Industry 4.0 scenarios brings along new security risks and widens the threat landscape.

The message is clear. Industry 4.0 and IoT create unique opportunities.

However, the challenges are also unique especially when it comes to cybersecurity.

The advanced digitisation envisaged in Industry 4.0 brings a paradigm shift and blurs the boundaries between the physical and digital world. This means that entities in the digital world can affect entities in the physical world. It is thus evident that the need for **cybersecurity becomes extremely important because it also has an impact on safety.**

---

[1] See https://www.pwc.nl/en/assets/documents/pwc-industrie-4-0.pdf, January 2015
[2] See https://www.bcg.com/publications/2015/engineered_products_project_business_industry_4_future_productivity_growth_manufacturing_industries.aspx, April 2015

- In May and August 2017, two different pieces of research showed that it is feasible to attack **automated industrial robots since they were vulnerable to cyber-attacks**[3].
- In October 2016, the **Mirai botnet**, which comprised hundreds of thousands of compromised IoT devices, was used to **take down major Internet services and operators** in a massive DDoS attack[4].
- In May 2017, **car factories and other manufacturing industries** were victims of one of the biggest ransomware attacks ever recorded, **Wannacry**[5].

With a great impact on citizens' safety, security and privacy due to its cyber-physical nature, the threat landscape concerning Industry 4.0 and IoT is extremely wide.

We need to be sure that all of these intelligent, connected products will operate in a secure and safe manner.

We need to trust that our autonomous vehicle will stop if an obstacle appears in front of them.

We need to trust that a robot in a smart factory is operating as it should be and is not harming anybody in any way.

At ENISA we don't believe that cybersecurity should only come as a result of being afraid of losing money. At ENISA we believe that it is important, for Europe and for European businesses, to **not look at cybersecurity only as a cost, but to also start seeing it as an important opportunity**. Europe is known for being reliable and trustworthy and for delivering high quality products. Cybersecurity can be an important competitive advantage for European businesses.

Cybersecurity is an enabler of business opportunities, not a hindering factor and certainly not another item on a checklist.

In the context of IoT and Industry 4.0 cybersecurity is particularly prominent:

- Because **consumers** need to have trust in the secure operation of their devices and products.
- Because **industries** need to have guarantees that their operations will remain unaffected.
- Because **countries** need to have safeguards in place to ensure that their critical infrastructures and services are not subject to IoT security shortcomings.

The need to secure IoT and Industry 4.0 is clear; but how?

The complexity of the IoT ecosystem and its many different aspects make it difficult to establish safeguards and ensure acceptable levels of security. There is no silver bullet. We advocate for holistic approaches, covering all elements of the Industry 4.0 landscape and addressing the needs of all the stakeholders involved.

---

[3] See http://blog.ioactive.com/2017/08/Exploiting-Industrial-Collaborative-Robots.html and https://www.ft.com/content/1552b080-fe1c-11e6-8d8e-a5e3738f9ae4, August 2017
[4] See https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers, October 2017
[5] See https://www.carscoops.com/2017/06/wannacry-ransomware-virus-shuts-down/, June 2017

Cybersecurity is a shared responsibility. And when we talk about IoT and Industry 4.0, with complex supply chains and several actors involved, this is even more true.

To improve the cybersecurity posture of Industry 4.0, we have to consider an array of solutions:

- To **improve the baseline security** of connected IoT devices.
- To **establish cybersecurity culture** in organisations.
- To formulate and promote a set of **principles on cyber ethics**.
- To set up **schemes to support and built trust on secure Industry 4.0** products and services.

ENISA has been working and continues to work on strengthening IoT cybersecurity. We do this by working with the European Commission, the Member States and the private sector. ENISA hosts a big conference on IoT Security every year and the next one is scheduled for the coming October. Moreover, the European Cybersecurity Month has one week dedicated on IoT Security.

A few months ago, we published a comprehensive study on Baseline Security Recommendations for IoT[6]. This study aims to set the scene for IoT cybersecurity in Europe. Based on its findings we have identified the need to:

- Raise awareness for IoT cybersecurity.
- Foster economic and administrative incentives for IoT security.
- Clarify relevant liability concerns.

Cybersecurity is the springboard for a safer and more resilient connected world.

ENISA is here to raise awareness and raise the bar for cybersecurity in Europe, promoting the much needed cybersecurity culture and advocating for cyber hygiene and cyber ethics.

The European Commission has identified cybersecurity as one of its major strategic objectives.

In 2016, **the first piece of EU-wide cybersecurity legislation was adopted.** As part of an EU-wide cybersecurity strategy, the European Commission proposed an EU directive on cybersecurity, namely the Network and Information Security (NIS) Directive, to **improve information sharing and collaboration across the EU.**

ENISA has an important role in the NIS Directive and we are currently working with the Commission and the EU Member States towards the implementation of the NIS Directive.

In particular, ENISA:

- **Leverages its existing knowledge and expertise** in the sectors mentioned in the NIS Directive.
- **Contributes to the implementation of the Directive** by engaging stakeholders, develops baseline security requirements and contributes to EU-wide harmonisation of incident reporting mechanisms.
- **Provides the secretariat for the CSIRT Network and contributes in the Cooperation group.**

[6] See https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot, November 2017

Realizing the potential of ENISA and the need for it to be stronger, in 2017 the European Commission proposed the Cybersecurity act, a Regulation that aims at further increasing EU cyber resilience, deterrence and defence. The Regulation proposal builds on two pillars:

1. A permanent and stronger mandate for ENISA to assist Member States in effectively preventing and responding to cyber-attacks; and
2. The creation of a European cybersecurity certification framework to ensure that ICT products and services meet certain cybersecurity requirements.

Harmonising cybersecurity certification approaches at European level can **increase the transparency of information on the security level of ICT products and services** in the digital single market for all its participants.

The proposed certification framework will provide **EU-wide certification schemes** as a comprehensive set of rules, technical requirements, standards and procedures. This will rely on agreement at EU level for the evaluation of the security properties of specific ICT-based products, services or even processes.

By undergoing a certification process, we will be able to **attest** that ICT products and services **meet specific cybersecurity requirements**. The resulting certificate will be recognized in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of products and services. Should these cybersecurity requirements are based on internationally accepted standards, the resulting certificate would also provide a certain level of assurance outside EU.

We believe that different business sectors across the EU will benefit from the provisions of the Cybersecurity act and the proposed certification framework in particular. Allow me to explain, and give you three reasons:

First, a new market opens up for businesses and industries. The opportunities and the technicalities regarding ICT products and services certification will open up the market to new players and require additional efforts from existing ones.

Second, the harmonised EU wide certification framework will inherently promote the cross-border flow and exchange of secure ICT products and services, based on the security by design paradigm. Businesses will be able to deal with a homogeneous system and thus require less resources in dealing with diverse compliance schemes.

Third, the level of consumer trust that will be brought by the new certification framework and the strong willingness of the EU to handle cybersecurity as a priority at a strategic level will boost the confidence of consumers in EU products. And this not only affects the EU internal market, but also the global one.

Another important provision of the Cybersecurity act involves the role of ENISA in supporting sectorial **Information Sharing and Analysis Centers (ISACs)** and **Public Private Partnerships (PPPs)**. The importance of involving both the public and the private sector and establishing trust relationships between industries and other stakeholders is evident. And it becomes even more important in the complex Industry 4.0 ecosystem with many players involved.

ENISA has been working on the topic and recently published two dedicated studies on cooperative models for ISACs and PPPs highlighting relevant challenges, but more importantly providing recommendations on the developments of such initiatives.

In the case of Industry 4.0 and IoT and relevant cybersecurity schemes in the EU, there are several questions to ponder:

- What would be the scope of a possible IoT cybersecurity certification scheme? For example, the devices, the networks, the protocols, all of the above?
- Do the same security measures apply when a smart connected device, e.g. smart coffee maker, is located in one's home and when it is located in a nuclear power plant?
- What will be the benchmark against which potential cybersecurity schemes will be defined? Do we set minimum requirements and if so based on which best practices?
- How can experience and expertise be drawn from international standards and existing initiatives?
- Does industry get value out of certification? When is the Return On Investment (ROI) positive and when does it not work?
- How can we make consumers aware of the cybersecurity characteristics of each product or service?

There is no one size fits all solution for IoT and Industry 4.0 security. It is a matter of combining solutions and ensuring that these solutions cater for flexibility and extensibility without sacrificing security and transparency.

Let me sum up by saying the following.

By being secure, we can be safer, we can be better.

And we need to be better, we need to be safer, we need to be more secure.

Especially in the context of Industry 4.0 and IoT, it is important to note that international cooperation and coordination efforts are much needed. The interconnections and interdependencies that these new technologies enable transcend borders and boundaries in both the physical and the digital world.

At the EU Cybersecurity Agency, ENISA, we support the EU in its path towards a more secure future. In doing so, we work together with policy makers and industry to make sure that cybersecurity is an enabler of, and not a barrier to economic progress.

Thank you for your attention.

ENISA

European Union Agency for Network
and Information Security

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu